

Hacking Articles

Raj Chandel's Blog



Menu

[Home](#) » [Penetration Testing](#) » [Comprehensive Guide on Dirsearch \(Part 2\)](#)

Penetration Testing

Comprehensive Guide on Dirsearch (Part 2)

February 13, 2021 By Raj Chandel

This is the second instalment of our series comprehensive guide on dirsearch. In the first part of this series, we have discussed some basic command on dirsearch. If you haven't checked the first part yet you can learn these features from [here](#). In this part, we will try to explore some more option of this command-line tool dirsearch.

Table of Content

- URL Attack
- Full URL
- Exclude Status Codes
- Minimal Size
- Maximal Size
- Random Agent
- Include Status Code
- Suffixes
- Prefixes
- Threads
- Only Selected
- Remove Extensions

- Upper Case Directories
- Lower Case Directories
- Capital Letter Directories
- Exclude Text
- Exclude Sizes

URL Attack

Firstly, we are taking the reference for simple URL attack. With the help of the [-u] parameter, we can use our web content scanner on a particular targeted URL. To get the required results, we need to ensure that this command is accompanied by an authenticated URL to get the desired results.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/
```

As we can see we got some web directories and web pages. In this screenshot, we have highlighted a few things. Like default extensions [php, aspx, jsp, html, js], default HTTP method [GET], default Threads [30] and default wordlist size [10832]. These things act very crucially in our directories attack and we are tacking these as a reference from time to time in our attack.

```
(root@kali)-[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/

dirsearch v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10832

Error Log: /root/dirsearch/logs/errors-21-02-04_14-52-37.log

Target: http://testphp.vulnweb.com/

Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-02-04_14-52-38.txt

[14:52:38] Starting:
[14:52:46] 200 - 6B - /.idea/.name
[14:52:46] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[14:52:46] 200 - 951B - /.idea/
[14:52:47] 200 - 171B - /.idea/encodings.xml
[14:52:47] 200 - 143B - /.idea/scopes/scope_settings.xml
[14:52:47] 200 - 275B - /.idea/modules.xml
[14:52:47] 200 - 266B - /.idea/misc.xml
[14:52:47] 200 - 12KB - /.idea/workspace.xml
[14:52:47] 200 - 173B - /.idea/vcs.xml
[14:52:55] 200 - 5KB - /404.php
[14:52:56] 200 - 595B - /CVS/
[14:52:56] 200 - 1B - /CVS/Root
[14:52:56] 200 - 1B - /CVS/Entries
[14:52:56] 301 - 169B - /Connections → http://testphp.vulnweb.com/Connections/
[14:53:02] 200 - 400B - /_mmServerScripts/
[14:53:02] 200 - 93B - /_mmServerScripts/MMHTTPDB.php
[14:53:05] 301 - 169B - /admin → http://testphp.vulnweb.com/admin/
[14:53:05] 200 - 262B - /admin/
```

Full URL

Sometimes these directories attack results can be confusing. To solve these confusions, we have a separated parameter called `[-full-url]`. This parameter helps us to gone through these results with ease.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ --full-url
```

As we can see from these results, we have got full url details now.

```
(root@kali)~[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ --full-url

cli-5 (z-cii-ct) v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10832
Error Log: /root/dirsearch/logs/errors-21-01-29_12-24-46.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_12-24-47.txt

[12:24:47] Starting:
[12:24:52] 301 - 169B - http://testphp.vulnweb.com/.idea → http://testphp.vulnweb.com/.idea/
[12:24:52] 200 - 951B - http://testphp.vulnweb.com/.idea/
[12:24:52] 200 - 171B - http://testphp.vulnweb.com/.idea/encodings.xml
[12:24:52] 200 - 266B - http://testphp.vulnweb.com/.idea/misc.xml
[12:24:52] 200 - 143B - http://testphp.vulnweb.com/.idea/scopes/scope_settings.xml
[12:24:52] 200 - 6B - http://testphp.vulnweb.com/.idea/.name
[12:24:52] 200 - 173B - http://testphp.vulnweb.com/.idea/vcs.xml
[12:24:52] 200 - 12KB - http://testphp.vulnweb.com/.idea/workspace.xml
[12:24:52] 200 - 275B - http://testphp.vulnweb.com/.idea/modules.xml
[12:24:57] 200 - 5KB - http://testphp.vulnweb.com/404.php
[12:24:58] 200 - 595B - http://testphp.vulnweb.com/CVS/
[12:24:58] 200 - 1B - http://testphp.vulnweb.com/CVS/Root
[12:24:58] 200 - 1B - http://testphp.vulnweb.com/CVS/Entries
[12:24:58] 301 - 169B - http://testphp.vulnweb.com/Connections → http://testphp.vulnweb.c
```

Exclude Status Code

We know that, in five groups or divisions, all HTTP response status codes are segregated. The first digit of the status code determines the answer class, while there is no classifying or categorizing function for the last two digits.

There are five classes defined by their standards.

Code	Meaning	
1xx	Informational response	The request was received, continuing process.
2xx	Successful	The request was successfully received, understood, and accepted.
3xx	Redirection	Further action needs to be taken in order to complete the request.
4xx	Client Error	The request contains bad syntax or cannot be fulfilled.
5xx	Server Error	The server failed to fulfill an apparently valid report.

We can exclude this status code with our parameter called [-x]. Through this feature, we can remove the unwanted codes and get our desired results, get only those status which we wanted in our attack schedule.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -x 301
```

We can also exclude more than one status code by separating them with comma [.,].

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -x 301,302,403
```

As we can see in our results for this attack, we only get a successful one due to our parameter.

```

(root@kali)~[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -x 301,302,403

cli-5 02-01-2024 v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 |
Error Log: /root/dirsearch/logs/errors-21-01-29_12-32-20.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_12-32-20.log

[12:32:20] Starting:
[12:32:25] 200 - 951B - /.idea/
[12:32:25] 200 - 266B - /.idea/misc.xml
[12:32:25] 200 - 275B - /.idea/modules.xml
[12:32:25] 200 - 6B - /.idea/.name
[12:32:25] 200 - 143B - /.idea/scopes/scope_settings.xml
[12:32:25] 200 - 173B - /.idea/vcs.xml
[12:32:25] 200 - 12KB - /.idea/workspace.xml
[12:32:25] 200 - 171B - /.idea/encodings.xml
[12:32:30] 200 - 5KB - /404.php
[12:32:31] 200 - 595B - /CVS/
[12:32:31] 200 - 1B - /CVS/Entries
[12:32:31] 200 - 1B - /CVS/Root
[12:32:35] 200 - 93B - /_mmServerScripts/MMHTTPDB.php
[12:32:35] 200 - 400B - /_mmServerScripts/
[12:32:38] 200 - 262B - /admin/
[12:32:38] 200 - 262B - /admin/?/login
[12:32:48] 200 - 5KB - /cart.php
[12:32:51] 200 - 224B - /crossdomain.xml
[12:32:55] 200 - 894B - /favicon.ico
[12:32:58] 200 - 377B - /images/
[12:32:58] 200 - 3KB - /index.bak
[12:32:58] 200 - 5KB - /index.php
[12:32:58] 200 - 3KB - /index.zip
[12:33:01] 200 - 5KB - /login.php
[12:33:01] 200 - 5KB - /logout.php
[12:33:11] 200 - 5KB - /search.php
[12:33:12] 200 - 6KB - /signup.php

Task Completed

```

Minimal Size

Sometime some web pages have lots of small size files. These files have no use for us in offensive purposes so this tool provides us the power to eliminate them with `[-minimal]` parameter. We just need to specify the size in bytes, which we don't want in our results.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -x 301,302,403 --minimal=2048
```

As we can see in results it is showing only the successful results [due to `-x` parameter] with minimal size set by us which is 2kb or 2048 bytes.

```
(root@kali)~[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -x 301,302,403 --minimal=2048

cli-5 0_0-5-5 v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size
Error Log: /root/dirsearch/logs/errors-21-01-29_12-36-23.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_12-36-23.txt

[12:36:23] Starting:
[12:36:28] 200 - 12KB - /.idea/workspace.xml
[12:36:33] 200 - 5KB - /404.php
[12:36:52] 200 - 5KB - /cart.php
[12:37:10] 200 - 5KB - /index.php
[12:37:10] 200 - 3KB - /index.bak
[12:37:10] 200 - 3KB - /index.zip
[12:37:12] 200 - 5KB - /login.php
[12:37:12] 200 - 5KB - /logout.php
[12:37:21] 200 - 5KB - /search.php
[12:37:22] 200 - 6KB - /signup.php

Task Completed
```

Maximal Size

Wise versa of minimal size, maximal size is used to set the upper limit of the results. The parameter we use to achieve this is `[-maximal]`. We just need to specify the size in bytes, which we don't want in our results.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -x 301,302,403 --maximal=5120
```

We can also provide both minimal and maximal size together, this provides us with a proper range through which we can get a proper scope finding a particular size file.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -x 301,302,403 --minimal=2048 --
    maximal=5120
```

```
(root@kali)~[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -x 301,302,403 --minimal=2048 --maximal=5120

cli-5 7_5 7_5 v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10832
Error Log: /root/dirsearch/logs/errors-21-01-29_12-40-04.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_12-40-05.txt

[12:40:05] Starting:
[12:40:45] 200 - 5KB - /cart.php
[12:40:55] 200 - 5KB - /index.php
[12:40:55] 200 - 3KB - /index.zip
[12:40:55] 200 - 3KB - /index.bak
[12:41:01] 200 - 5KB - /logout.php
[12:41:11] 200 - 5KB - /search.php

Task Completed
```

Random Agent

We all recognize that a user agent in computing is a program (a software agent) that operates on behalf of a user, such as a web browser that “retrieves, renders, and facilitates interaction with web content by end-users.”

We can use the random user agent to break the default schedules and get our data results in the brand new order.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -x 301,302,403 --random-agent
```

```
(root@kali)-[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -x 301,302,403 --random-agent

cli--_o_c_--(+) v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 1000
Error Log: /root/dirsearch/logs/errors-21-01-29_12-46-50.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_12-46-50.txt

[12:46:50] Starting:
[12:46:54] 200 - 951B - /.idea/
[12:46:55] 200 - 171B - /.idea/encodings.xml
[12:46:55] 200 - 266B - /.idea/misc.xml
[12:46:55] 200 - 143B - /.idea/scopes/scope_settings.xml
[12:46:55] 200 - 275B - /.idea/modules.xml
[12:46:55] 200 - 173B - /.idea/vcs.xml
[12:46:55] 200 - 6B - /.idea/.name
[12:46:55] 200 - 12KB - /.idea/workspace.xml
[12:47:01] 200 - 5KB - /404.php
[12:47:02] 200 - 595B - /CVS/
[12:47:02] 200 - 1B - /CVS/Entries
```

Include Status Code

As we earlier performed exclude status code which would remove the unwanted status code. Include code is just likewise versa in this parameter we include any status code, which we want in our results.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200
```

We can include more than one status code, by just following this command.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200,301,302
```

As we can observe these results, it only shows these codes [200, 301, 302].


```

(root@kali)-[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200,301,302

cli-3 02-11-21 v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist
Error Log: /root/dirsearch/logs/errors-21-01-29_12-55-30.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_12-55-31.txt

[12:55:31] Starting:
[12:55:36] 301 - 169B - /.idea → http://testphp.vulnweb.com/.idea/
[12:55:36] 200 - 951B - /.idea/
[12:55:36] 200 - 6B - /.idea/.name
[12:55:36] 200 - 171B - /.idea/encodings.xml
[12:55:36] 200 - 266B - /.idea/misc.xml
[12:55:36] 200 - 275B - /.idea/modules.xml
[12:55:36] 200 - 143B - /.idea/scopes/scope_settings.xml
[12:55:37] 200 - 12KB - /.idea/workspace.xml
[12:55:37] 200 - 173B - /.idea/vcs.xml
[12:55:41] 200 - 5KB - /404.php
[12:55:42] 200 - 595B - /CVS/
[12:55:42] 200 - 1B - /CVS/Entries
[12:55:42] 200 - 1B - /CVS/Root
[12:55:42] 301 - 169B - /Connections → http://testphp.vulnweb.com/Connections
[12:55:45] 200 - 400B - /_mmServerScripts/
[12:55:45] 200 - 93B - /_mmServerScripts/MMHTTPDB.php
[12:55:47] 301 - 169B - /admin → http://testphp.vulnweb.com/admin/
[12:55:48] 200 - 262B - /admin/
[12:55:48] 200 - 262B - /admin/?/login
[12:55:58] 200 - 5KB - /cart.php
[12:56:01] 200 - 224B - /crossdomain.xml
[12:56:08] 200 - 894B - /favicon.ico
[12:56:10] 301 - 169B - /images → http://testphp.vulnweb.com/images/
[12:56:10] 200 - 377B - /images/
[12:56:10] 200 - 5KB - /index.php
[12:56:10] 200 - 3KB - /index.bak
[12:56:11] 200 - 3KB - /index.zip
[12:56:13] 200 - 5KB - /login.php
[12:56:13] 200 - 5KB - /logout.php
[12:56:18] 301 - 169B - /pictures → http://testphp.vulnweb.com/pictures/
[12:56:21] 200 - 5KB - /search.php
[12:56:22] 301 - 169B - /secured → http://testphp.vulnweb.com/secured/
[12:56:23] 200 - 6KB - /signup.php
[12:56:28] 302 - 14B - /userinfo.php → login.php

Task Completed

```

Suffixes

The grammatically meaning of a suffix. It is a letter or group of letters inserted at the end of a word that creates a new word. This parameter helps us to search only those specific result, which matches our provided suffix to the attack. To get these results in our attack.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ --suffixes=.php
```

As we can see these results, we successfully got all those results related through our provided suffix.

```
(root@kali)-[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ --suffixes=.php

dirsearch v0.4.1

Extensions: php, aspx, jsp, html, js | Suffixes: .php | HTTP method: GET | Threads: 30
Wordlist size: 8094

Error Log: /root/dirsearch/logs/errors-21-01-29_13-09-58.log

Target: http://testphp.vulnweb.com/

Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_13-09-58.txt

[13:09:58] Starting:
[13:10:00] 400 - 157B - /%2e%2e//google.com.php
[13:10:06] 200 - 5KB - /404.php
[13:10:11] 200 - 262B - /admin/?/login.php
[13:10:18] 200 - 5KB - /cart.php
[13:10:18] 200 - 6KB - /categories.php
[13:10:19] 302 - 1KB - /comment.php → ./index.php
[13:10:22] 200 - 5KB - /disclaimer.php
[13:10:26] 200 - 5KB - /index.php
[13:10:28] 200 - 5KB - /login.php
[13:10:28] 200 - 5KB - /logout.php
[13:10:34] 200 - 5KB - /product.php
[13:10:36] 200 - 5KB - /search.php
[13:10:37] 200 - 6KB - /signup.php

Task Completed
```

Prefixes

The grammatically meaning of a prefix. It is a letter or group of letters inserted at the start of a word that creates a new word. This parameter helps us to search only those specific result, which matches our provided prefix to the attack. To get these results in our attack.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ --prefixes=index
```

As we can see these results, it is only showing those results which have our prefixes.

```
(root@kali)-[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ --prefixes=index

dirsearch v0.4.1

Extensions: php, aspx, jsp, html, js | Prefixes: index | HTTP method: GET | Threads: 30
Wordlist size: 10776

Error Log: /root/dirsearch/logs/errors-21-01-29_13-12-53.log

Target: http://testphp.vulnweb.com/

Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_13-12-54.txt

[13:12:54] Starting:
[13:12:56] 200 - 3KB - /index.bak
[13:12:59] 200 - 5KB - /index.php
[13:13:01] 200 - 3KB - /index.zip

Task Completed
```

Threads

We can increase or decrease the number of threads. This will increase or decrease the speed of our attack depending upon the number of threads provided by us. As we see earlier in URL attack the by **default number threads are set on 30**.

As we want to increase the speed of attack so we change it to **100** with the help of [-t] parameter.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 -t 100
```

```
(root@kali)-[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 -t 100

dirsearch v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 |
Error Log: /root/dirsearch/logs/errors-21-01-29_13-19-24.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_13-19-

[13:19:25] Starting:
[13:19:27] 200 - 6B - /.idea/.name
[13:19:27] 200 - 951B - /.idea/
[13:19:27] 200 - 275B - /.idea/modules.xml
[13:19:27] 200 - 266B - /.idea/misc.xml
[13:19:27] 200 - 173B - /.idea/vcs.xml
[13:19:28] 200 - 143B - /.idea/scopes/scope_settings.xml
[13:19:28] 200 - 171B - /.idea/encodings.xml
[13:19:28] 200 - 12KB - /.idea/workspace.xml
[13:19:29] 200 - 5KB - /404.php
[13:19:29] 200 - 595B - /CVS/
[13:19:29] 200 - 1B - /CVS/Root
[13:19:29] 200 - 1B - /CVS/Entries
[13:19:31] 200 - 400B - /_mmServerScripts/
[13:19:31] 200 - 93B - /_mmServerScripts/MMHTTPDB.php
[13:19:32] 200 - 262B - /admin/
[13:19:32] 200 - 262B - /admin/?/login
[13:19:37] 200 - 5KB - /cart.php
[13:19:38] 200 - 224B - /crossdomain.xml
[13:19:39] 200 - 894B - /favicon.ico
[13:19:40] 200 - 5KB - /index.php
[13:19:40] 200 - 377B - /images/
[13:19:40] 200 - 3KB - /index.zip
[13:19:40] 200 - 3KB - /index.bak
[13:19:40] 200 - 5KB - /login.php
[13:19:40] 200 - 5KB - /logout.php
[13:19:43] 200 - 5KB - /search.php
[13:19:44] 200 - 6KB - /signup.php

Task Completed
```

Only selected

In this parameter called `[-only-selected]`, we got a focused directories wordlist through which only got selected web pages and directories. This can be very useful to find out some great results through the attack.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 --only-selected
```

As we can see in the banner of this tool our wordlist got shorter size **10832 to 7608**.

```
(root@kali)~[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 --only-selected

v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 7608

Error Log: /root/dirsearch/logs/errors-21-02-04_15-00-00.log

Target: http://testphp.vulnweb.com/

Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-02-04_15-00-00.txt

[15:00:00] Starting:
[15:00:03] 200 - 951B - /.idea/
[15:00:05] 200 - 5KB - /404.php
[15:00:06] 200 - 595B - /CVS/
[15:00:07] 200 - 1B - /CVS/Entries
[15:00:07] 200 - 1B - /CVS/Root
[15:00:12] 200 - 93B - /_mmServerScripts/MMHTTPDB.php
[15:00:12] 200 - 400B - /_mmServerScripts/
[15:00:16] 200 - 262B - /admin/
[15:00:16] 200 - 262B - /admin/?/login
[15:00:29] 200 - 5KB - /cart.php
[15:00:41] 200 - 377B - /images/
[15:00:42] 200 - 5KB - /index.php
[15:00:44] 200 - 5KB - /login.php
[15:00:45] 200 - 5KB - /logout.php
[15:00:57] 200 - 5KB - /search.php
[15:00:58] 200 - 6KB - /signup.php

Task Completed
```

Remove Extension

We all know the definition of the extension, a file extension (or simply “extension”) is the suffix at the end of a file name that specifies what sort of file it is. We can remove extension files from our results. To get this kind of results we can use our parameter called `[-remove-extensions]`.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 --remove-extensions
```

As we can see it removes all the extensions.

```
(root@kali)-[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 --remove-extensions

cli-5 02-01-29 v0.4.1

Extensions: HTTP method: GET | Threads: 30 | Wordlist size: 7007

Error Log: /root/dirsearch/logs/errors-21-01-29_13-46-01.log

Target: http://testphp.vulnweb.com/

Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_13-46-01.txt

[13:46:01] Starting:
[13:46:02] 200 - 5KB - /.
[13:46:05] 200 - 951B - /.idea/
[13:46:11] 200 - 595B - /CVS/
[13:46:11] 200 - 1B - /CVS/Entries
[13:46:11] 200 - 1B - /CVS/Root
[13:46:14] 200 - 400B - /_mmServerScripts/
[13:46:16] 200 - 262B - /admin/
[13:46:16] 200 - 262B - /admin/?/login
[13:46:33] 200 - 377B - /images/

Task Completed
```

Upper Case Directories

It just acts like a filter, which only let's go to the upper-case directories with the help of parameter [-U]. we can apply this filter by using this command.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -U
```

```
(root@kali)-[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -U

cli-5 02-01-29 v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 |

Error Log: /root/dirsearch/logs/errors-21-01-29_14-05-07.log

Target: http://testphp.vulnweb.com/

Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_14-05-07.log

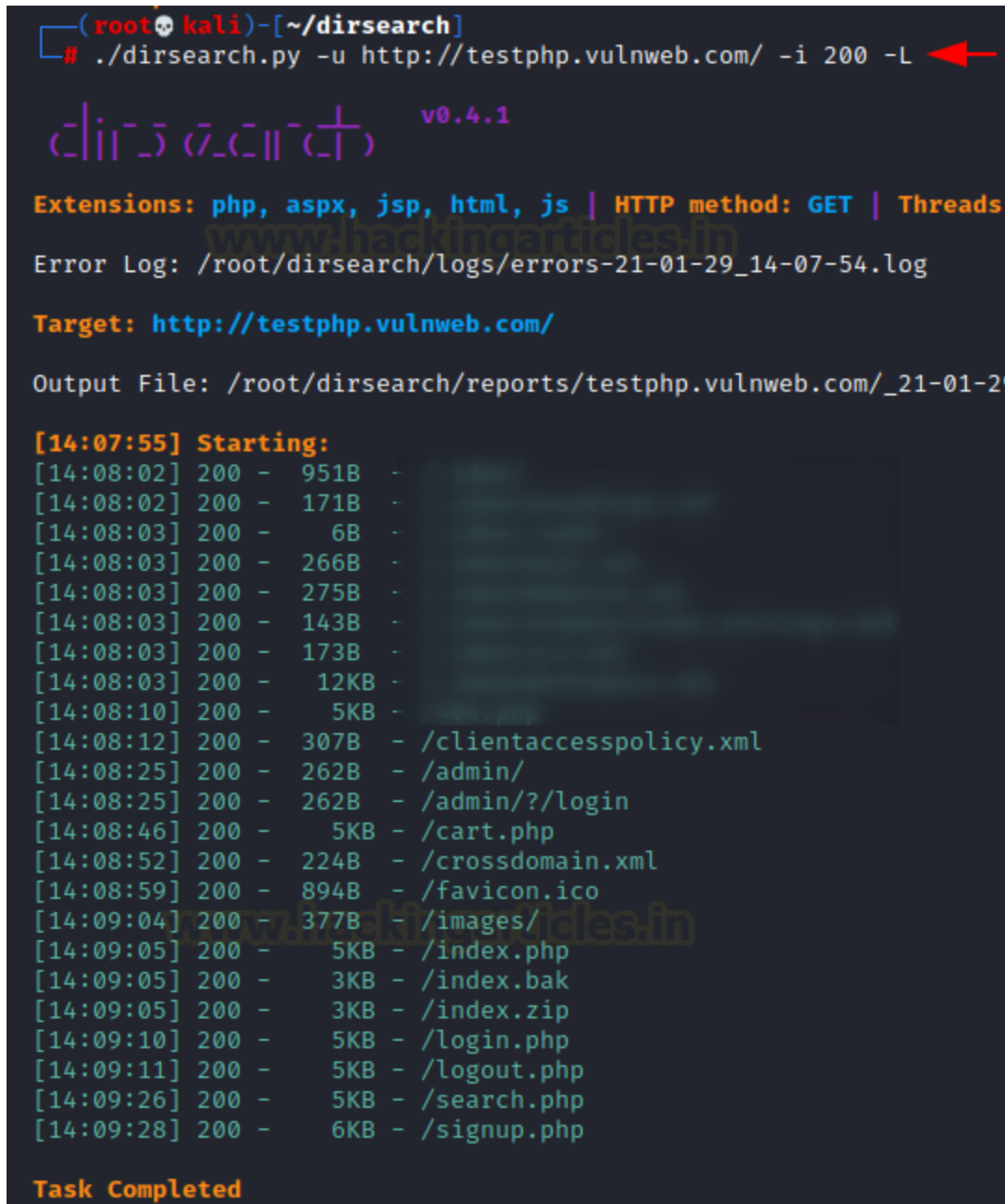
[14:05:07] Starting:
[14:05:10] 400 - 157B - /%2E%2E//GOOGLE.COM
[14:05:27] 200 - 595B - /CVS/
[14:05:49] 301 - 169B - /AJAX → http://testphp.vulnweb.com/AJAX/
[14:05:59] 301 - 169B - /CVS → http://testphp.vulnweb.com/CVS/

Task Completed
```

Lower Case Directories

Similarly, as above it is just like a filter. Which only let's go to the lower-case directories with the help of parameter [-L]. we can apply this filter by using this command.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 -L
```



```
(root@kali)~# ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 -L

dirsearch v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads
Error Log: /root/dirsearch/logs/errors-21-01-29_14-07-54.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_14-07-54.log

[14:07:55] Starting:
[14:08:02] 200 - 951B - /
[14:08:02] 200 - 171B - /
[14:08:03] 200 - 6B - /
[14:08:03] 200 - 266B - /
[14:08:03] 200 - 275B - /
[14:08:03] 200 - 143B - /
[14:08:03] 200 - 173B - /
[14:08:03] 200 - 12KB - /
[14:08:10] 200 - 5KB - /
[14:08:12] 200 - 307B - /clientaccesspolicy.xml
[14:08:25] 200 - 262B - /admin/
[14:08:25] 200 - 262B - /admin?/login
[14:08:46] 200 - 5KB - /cart.php
[14:08:52] 200 - 224B - /crossdomain.xml
[14:08:59] 200 - 894B - /favicon.ico
[14:09:04] 200 - 377B - /images/
[14:09:05] 200 - 5KB - /index.php
[14:09:05] 200 - 3KB - /index.bak
[14:09:05] 200 - 3KB - /index.zip
[14:09:10] 200 - 5KB - /login.php
[14:09:11] 200 - 5KB - /logout.php
[14:09:26] 200 - 5KB - /search.php
[14:09:28] 200 - 6KB - /signup.php

Task Completed
```

Capital Letter Directories

It acts as a filter, which only let's go the first letter capital directories with the help of parameter [-C]. we can apply this filter by using this command.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 -C
```

```
(root@kali)~[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 -C

dirsearch v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads
Error Log: /root/dirsearch/logs/errors-21-01-29_14-12-07.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_14-12-07.log

[14:12:07] Starting:
[14:12:13] 200 - 6B - /
[14:12:13] 200 - 951B - /css/
[14:12:13] 200 - 275B - /js/
[14:12:13] 200 - 143B - /images/
[14:12:13] 200 - 266B - /media/
[14:12:13] 200 - 171B - /plugins/
[14:12:13] 200 - 173B - /themes/
[14:12:13] 200 - 12KB - /wp-content/
[14:12:21] 200 - 5KB - /wp-includes/
[14:13:09] 200 - 371B - /Flash/
[14:13:36] 200 - 289B - /Templates/

Task Completed
```

Exclude Text

As earlier we have removed or excluded the unwanted status codes, we can also exclude some text from our results as per our need. By using this parameter called `[-exclude-texts]`.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 --exclude-texts=index
```

As we can see this result and compare it without filtered results, we can observe that it has excluded index text from its results.


```
(root@kali)~[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 --exclude-texts=index

cli-5 02-01-29 v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 1000
Error Log: /root/dirsearch/logs/errors-21-01-29_14-37-11.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_14-37-12.txt

[14:37:12] Starting:
[14:37:16] 200 - 6B - /.idea/.name
[14:37:16] 200 - 951B - /.idea/
[14:37:16] 200 - 171B - /.idea/encodings.xml
[14:37:16] 200 - 266B - /.idea/misc.xml
[14:37:16] 200 - 275B - /.idea/modules.xml
[14:37:16] 200 - 143B - /.idea/scopes/scope_settings.xml
[14:37:16] 200 - 173B - /.idea/vcs.xml
[14:37:16] 200 - 12KB - /.idea/workspace.xml
[14:37:21] 200 - 595B - /CVS/
[14:37:21] 200 - 1B - /CVS/Entries
[14:37:21] 200 - 1B - /CVS/Root
[14:37:25] 200 - 400B - /_mmServerScripts/
[14:37:25] 200 - 93B - /_mmServerScripts/MMHTTPDB.php
[14:37:27] 200 - 262B - /admin/
[14:37:27] 200 - 262B - /admin/?/login
[14:37:39] 200 - 224B - /crossdomain.xml
[14:37:42] 200 - 894B - /favicon.ico
[14:37:44] 200 - 377B - /images/

Task Completed
```

Exclude sizes

As earlier we have removed or excluded the unwanted text, we can also exclude some file sizes from our results as per our need. By using this parameter called `[-exclude-sizes]`.

```
1. ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 --exclude-sizes=5KB
```

As we can see this result and compare it without filtered results, we can observe that it has excluded files sizes have 5KB from its results.

```
(root@kali)~[~/dirsearch]
# ./dirsearch.py -u http://testphp.vulnweb.com/ -i 200 --exclude-sizes=5KB

c|ii-5 0_0ii-(t) v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist
Error Log: /root/dirsearch/logs/errors-21-01-29_14-35-15.log
Target: http://testphp.vulnweb.com/
Output File: /root/dirsearch/reports/testphp.vulnweb.com/_21-01-29_14-35-16.txt

[14:35:16] Starting:
[14:35:20] 200 - 6B - /.idea/.name
[14:35:20] 200 - 951B - /.idea/
[14:35:20] 200 - 266B - /.idea/misc.xml
[14:35:20] 200 - 275B - /.idea/modules.xml
[14:35:20] 200 - 171B - /.idea/encodings.xml
[14:35:20] 200 - 143B - /.idea/scopes/scope_settings.xml
[14:35:20] 200 - 173B - /.idea/vcs.xml
[14:35:20] 200 - 12KB - /.idea/workspace.xml
[14:35:25] 200 - 595B - /CVS/
[14:35:25] 200 - 1B - /CVS/Root
[14:35:25] 200 - 1B - /CVS/Entries
[14:35:29] 200 - 400B - /_mmServerScripts/
[14:35:29] 200 - 93B - /_mmServerScripts/MMHTTPDB.php
[14:35:31] 200 - 262B - /admin/
[14:35:31] 200 - 262B - /admin/?/login
[14:35:43] 200 - 224B - /crossdomain.xml
[14:35:46] 200 - 894B - /favicon.ico
[14:35:48] 200 - 377B - /images/
[14:35:49] 200 - 3KB - /index.bak
[14:35:49] 200 - 3KB - /index.zip
[14:36:00] 200 - 6KB - /signup.php

Task Completed
```

Author: Shubham Sharma is a passionate Cybersecurity Researcher, contact [LinkedIn](#) and [Twitter](#).

◀ PREVIOUS POST

WebDAV Penetration Testing

NEXT POST ▶

Remote HackTheBox Walkthrough

Join Our Training Program





Categories

Cryptography & Steganography

CTF Challenges

Cyber Forensics

Database Hacking

Footprinting

Hacking Tools

Kali Linux

Nmap

Others

Password Cracking

Penetration Testing

Pentest Lab Setup

Privilege Escalation

Red Teaming

Social Engineering Toolkit

Uncategorized

Website Hacking

Window Password Hacking

Wireless Hacking

Wireless Penetration Testing

Archives

Select Month



You may like

Best Alternative of Netcat Listener

April 3, 2024

64-bit Linux Assembly and Shellcoding

March 29, 2024